WHAT IS CLAIMED IS:

1. A method of providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in a Semi-Connected Mode (SCM), said method comprising the steps of:

establishing a first call from the mobile subscriber to a first access server;

establishing a point-to-point protocol (PPP) connection from the mobile subscriber to an Internet Protocol (IP)-based network through the first access server;

providing the mobile subscriber with an identifier for the first access server;

moving the connection to the SCM state when the mobile subscriber disconnects the first call;

receiving from the mobile subscriber, the identifier for the first access server, said identifier being received in a second access server that handles a subsequent call origination from the mobile subscriber to the IP-based network;

utilizing the identifier for the first access server to send from the second access server to the first access server, a Calling Number Identification (CNID) for the mobile subscriber;

establishing a PPP tunnel through the IP-based network between the first access server and the second access server;

tunnelling PPP packets from the second access server to the first access server; and

re-establishing the connection from the mobile subscriber to the IP-based network.

2. The method of claim 1, wherein the step of receiving the identifier for the first access server from the mobile subscriber includes receiving the identifier by the second access server utilizing the User-to-User Signalling (UUS) Supplementary Service before starting subsequent PPP setup.

3. The method of claim 2, wherein the step of providing the mobile subscriber with an identifier for the first access server also includes providing the mobile subscriber with a password that uniquely identifies the mobile subscriber if the mobile subscriber's CNID does not uniquely identify the mobile subscriber, and the method further comprises sending the password together with the CNID from the

second access server to the first access server, and utilizing the CNID by the first access server to look up and verify the password.

4. The method of claim 2, wherein the step of receiving the identifier for the first access server from the mobile subscriber includes receiving in the second access server, an IP address for the first access server.

5. The method of claim 1, wherein the step of establishing a connection from the mobile subscriber to the IP-based network includes sending a request to utilize the SCM from the mobile subscriber to the first access server.

6. The method of claim 1, wherein the step of establishing a connection from the mobile subscriber to the IP-based network includes determining by the first access server that the mobile subscriber is authorized to utilize the SCM.

7. The method of claim 1, wherein the step of providing the mobile subscriber with an identifier for the first access server also includes providing the mobile subscriber with a password that uniquely identifies the mobile subscriber if the mobile subscriber's CNID does not uniquely identify the mobile subscriber, and the method further comprises sending the password together with the CNID from the second access server to the first access server, and utilizing the CNID by the first access server to look up and verify the password.

8. A method of providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in a Semi-Connected Mode (SCM), said method comprising the steps of:

establishing a first call from the mobile subscriber to a first access server;

establishing a point-to-point protocol (PPP) connection from the mobile subscriber to an Internet Protocol (IP)-based network through the first access server;

providing the mobile subscriber with an identifier for the first access server;

moving the connection to the SCM state when the mobile subscriber disconnects the first call;

receiving from the mobile subscriber, the identifier for the first access server, said identifier being received in a second access server that handles a subsequent call origination from the mobile subscriber to the IP-based network;

analyzing by the second access server, the identifier for the first access server to determine whether the second access server is the first access server;

if the second access server is the first access server:

determining whether a Calling Number Identification (CNID) for the mobile subscriber is recognized;

if the CNID is recognized, re-establishing the connection from the mobile subscriber to the IP-based network; and

if the CNID is not recognized, starting a new PPP setup to establish a new connection from the mobile subscriber to the IP-based network;

if the second access server is not the first access server:

sending from the second access server to the first access server, the CNID for the mobile subscriber;

determining whether the CNID for the mobile subscriber is recognized by the first access server;

if the CNID is recognized, using the CNID by the first access server to look up SCM data for the connection, establishing a PPP tunnel through the IP-based network between the first access server and the second access server, tunnelling PPP packets from the second access server to the first access server, and re-establishing the connection from the mobile subscriber to the IP-based network; and

if the CNID is not recognized, sending a negative reply from the first access server to the second access server, and starting a new PPP setup by the second access server to establish a new connection from the mobile subscriber to the IP-based network.

9. The method of claim 8, wherein the step of receiving the identifier for the first access server from the mobile subscriber includes receiving the identifier by the second access server utilizing the User-to-User Signalling (UUS) Supplementary Service before starting subsequent PPP setup.

10. The method of claim 9, wherein the step of providing the mobile subscriber with an identifier for the first access server also includes providing the mobile subscriber with a password that uniquely identifies the mobile subscriber if the mobile subscriber's CNID does not uniquely identify the mobile subscriber, and the method further comprises sending the password together with the CNID from the second access server to the first access server, and utilizing the CNID by the first access server to look up and verify the password.

11. The method of claim 9, wherein the step of receiving the identifier for the first access server from the mobile subscriber includes receiving in the second access server, an IP address for the first access server.

12. The method of claim 8, wherein the step of providing the mobile subscriber with an identifier for the first access server also includes providing the mobile subscriber with a password that uniquely identifies the mobile subscriber if the mobile subscriber's CNID does not uniquely identify the mobile subscriber, and the method further comprises sending the password together with the CNID from the second access server to the first access server, and utilizing the CNID by the first access server to look up and verify the password.

13. A system for providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in a Semi-Connected Mode (SCM), said system comprising:

a first access server that establishes a call and a point-to-point protocol (PPP) connection from the mobile subscriber to an Internet Protocol (IP)-based network;

a second access server that handles a subsequent call origination from the mobile subscriber to the IP-based network; and

a PPP tunnel between the first access server and the second access server;

wherein the first access server includes:

communication means for providing the mobile subscriber with an identifier for the first access server; and

means controlled by a PPP state machine for placing the connection in a Semi-Connected state when the mobile subscriber disconnects the call, and for

placing the connection in a Network state when the mobile subscriber originates the subsequent call origination; and

wherein the second access server includes:

communication means for receiving the identifier for the first access server from the mobile subscriber, and for sending the Calling Number Identification (CNID) for the mobile subscriber from the second access server to the first access server; and

means for tunnelling PPP packets from the second access server to the first access server through the PPP tunnel;

whereby the connection from the mobile subscriber to the IP-based network is re-established.

14. The system of claim 13, wherein the communication means for receiving the identifier for the first access server from the mobile subscriber includes a signalling means that utilizes the User-to-User Signalling (UUS) Supplementary Service before starting subsequent PPP setup.

15. The system of claim 14, wherein the communication means for providing the mobile subscriber with an identifier for the first access server includes means for providing an IP address for the first access server to the mobile subscriber.

16. The system of claim 13, wherein the communication means for providing the mobile subscriber with an identifier for the first access server also provides the mobile subscriber with a password that uniquely identifies the mobile subscriber if the mobile subscriber's CNID does not uniquely identify the mobile subscriber, and the first access server further comprises a CNID-to-password lookup table for looking up and verifying that the password is associated with the CNID of the mobile subscriber.

17. A network access server for providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in a Semi-Connected Mode (SCM), said network access server comprising:

means for receiving a call origination request from the mobile subscriber, said request including a Calling Number Identification (CNID) for the mobile subscriber;

means for establishing a point-to-point (PPP) connection from the mobile subscriber to the network;

means for providing the mobile subscriber with an identifier for the network access server;

means for storing SCM data for the connection and moving the connection to the SCM state when the mobile subscriber disconnects from the network access server;

means for receiving from a subsequent access server, the CNID of the mobile subscriber when the mobile subscriber originates another call request through the subsequent access server;

means for retrieving the SCM data using the CNID of the mobile subscriber; and

means for setting up a PPP tunnel through the network to the subsequent access server, said PPP tunnel re-establishing the connection from the mobile subscriber to the network by tunnelling PPP packets from the subsequent access server to the network access server.

18. The network access server of claim 17, further comprising:

means for determining whether the CNID for the mobile subscriber is recognized; and

means for sending a negative reply from the network access server to the subsequent access server if the CNID is not recognized.

19. A network access server for providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in a Semi-Connected Mode (SCM), said network access server comprising:

means for receiving a call origination request from the mobile subscriber, said request including a Calling Number Identification (CNID) for the mobile subscriber and an identifier for a previous access server through which a point-to-point (PPP) connection was previously established from the mobile subscriber to the network;

means for sending from the network access server to the previous access server, the CNID for the mobile subscriber; and

means for setting up a PPP tunnel through the network to the previous access server in response to a request from the previous access server, said PPP tunnel re-establishing the connection from the mobile subscriber to the network by tunnelling PPP packets from the network access server to the previous access server.

20. The network access server of claim 19, further comprising:

means for analyzing the identifier for the previous access server to determine whether the network access server is the previous access server;

means for determining whether the CNID for the mobile subscriber is recognized, upon determining that the network access server is the previous access server;

means for re-establishing the connection from the mobile subscriber to the network if the CNID is recognized; and

means for starting a new PPP setup to establish a new connection from the mobile subscriber to the network if the CNID is not recognized.